Comment crypter vos e−mails

.......hQIOA6lJ0QL4d+KakvBGyh0xE4nT3xtarGkGeoI0tCCiq+L+Q5D3AHUSV/
5GcCaNCMP5KEJUWUjzYqeJB4r1x8UlVdjfxpD515g0uGyO/PSlv2ahvsqzT6VH/V
U3OwXjEskvuzZqIs1PQVwTwsIVUM06pU+Fg/yBPrZHXEBhLhxV3aKufR71sfsA6h
lyR3tfWdy/6rYaICl6ZC3RAVbIqg3MTKj1uT3yNnLQf+PowCxdoSpZM1SLgHrRas
Ysdkuwi/xaJo8B2SuCI2b6czL5kKJ6PHsL58HhBct8HRK3ArODKqmU56K........

Ce document en version PDF

1. Pourquoi crypter vos e−mails?

1.1 Itinéraire d'un e−mail

Vos e−mails cheminent sur Internet par copies successives

Les e−mails se déplacent sur Internet par le biais de copies successives d'un serveur Internet (ordinateur du fournisseur d'accès à Internet (FAI)) à un autre serveur Internet.

Si vous habitez à Paris 6e et envoyez un e−mail à un correspondant qui habite à Paris 11e, voici les copies qui vont se créer :

Votre ordinateur (**copie originale**) −> un premier ordinateur chez votre fournisseur d'accès (**copie 1**) −> un second ordinateur chez votre fournisseur d'accès (**copie 2**) −> un premier ordinateur chez le fournisseur d'accès de votre destinataire (**copie 3**) −> un second ordinateur chez le fournisseur d'accès de votre destinataire (**copie 4**) −> l'ordinateur de votre correspondant (**copie chez le destinataire**).

Pour traverser trois arrondissements de Paris, ce e−mail a été inscrit au moins quatre fois sur quatre disques durs différents (quatre serveurs Internet chez les FAI) en autant de **copies parfaites.** Et derrière chacun de ces quatre disques durs, se cachent des entreprises commerciales, des informaticiens curieux, des administrations publiques diverses et variées...

Ces copies multiples de vos e−mails étaient jusqu'ici en théorie effacées au bout de quelques heures par chaque fournisseur d'accès. Cependant, de nouvelles législations européennes contre le "cyber" crime prévoient la conservation de ces copies pendant un an.

Un e−mail qui n'a pas été "crypté" (*) et est envoyé sur Internet est comme une carte postale sans enveloppe : les postiers, le facteur, la concierge, les voisins, peuvent lire la carte postale dans votre dos...

1.2 Confidentialités multiples, secret professionnel, vie privée et intimité

On ne saurait trop rappeler que l'utilisation de cryptographie sert non seulement à protéger votre confidentialité, mais aussi celle de vos correspondants.

1.2.1 Secrets non liés aux personnes : négociations, finances, justice

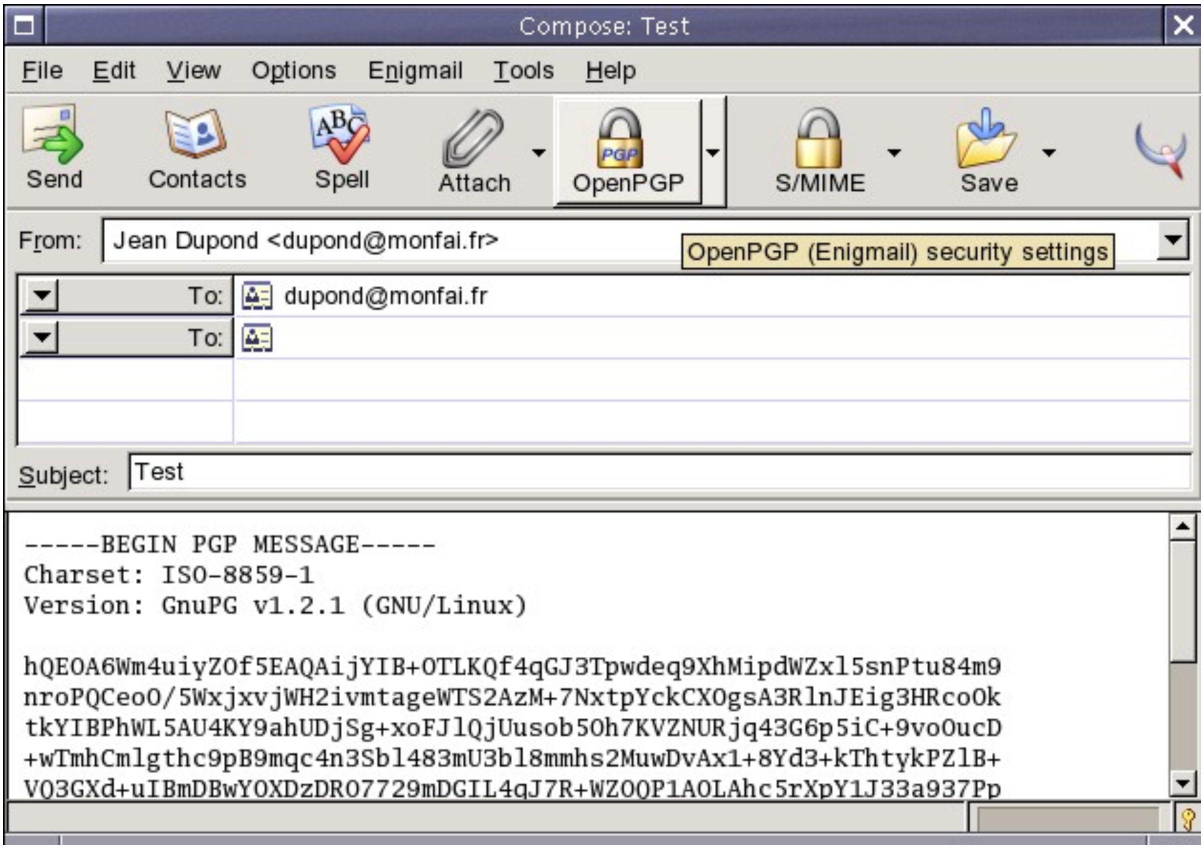
Journalistes, avocats, huissiers, médecins, cadres commerciaux... nombreux sont les professionnels qui, contractuellement, déontologiquement, ou légalement, sont tenus au **secret professionnel**. Ils sont aussi de plus en plus nombreux à utiliser l'internet de façon professionnelle. Ils sont donc dans l'obligation de crypter leurs e−mails afin de ne pas laisser se diffuser librement dans les labyrinthes d'Internet une proposition commerciale, un dossier judiciaire ou un dossier médical.

S'ils ne cryptent pas, ils ne prennent pas les précautions minimales pour préserver ce secret professionnel et s'exposent alors à des risques juridiques et financiers considérables.

1.2.2 Secrets liés aux personnes : vie privée, intimité, sentiments, famille

Vous ne cryptez pas car vous savez n'avoir "rien à cacher" ? Certes, mais cependant vous vous préoccupez de votre intimité, puisque lorsque vous êtes dans votre appartement, vous **tirez les rideaux des fenêtres**.

Vous n'aimeriez pas qu'**un inconnu** assis derrière les ordinateurs de votre fournisseur d'accès à Internet sourit en lisant à ses heures perdues les e−mails que vous échangez avec votre petit(e) ami(e). Si vous n'avez pas crypté vos e−mails, un inconnu a peut−être déjà lu ce que vous écriviez...



Message crypté au **format OpenPGP** (Thunderbird Mail)

2. Principe de base : le cadenas, et la clé du cadenas

Tout le monde possède le cadenas, mais vous seul possédez la clé du cadenas.

On appelle ce système la **cryptographie à clé publique**. Le programme de cryptographie à clé publique le plus connu est PGP© (pour "Pretty Good Privacy", en anglais : *"Assez Bonne Confidentialité"*).

Le format **OpenPGP** est le standard de cryptographie issu de PGP©. OpenPGP est un standard ouvert ("open"). Il est considéré par les cryptographes comme le plus sûr des procédés de cryptage pour e−mails.

OpenPGP est adopté par deux logiciels : **GPG** (gratuit) et **PGP**© (payant).
GPG et PGP© sont compatibles l'un avec l'autre.

OpenPGP fonctionne avec un **cadenas** (dite clé publique), et une **clé** (dite clé privée ou secrète) :
− votre cadenas est public
− la clé qui ouvre votre cadenas est secrète : vous êtes le seul à détenir cette clé.

2.1 Cryptage d'un message : on ferme le "cadenas" (clé PGP du destinataire)

Lorsque vous envoyez un message crypté, vous fermez le cadenas : vous cliquez sur l'**icône OpenPGP** du logiciel e−mail et le message va être automatiquement crypté avec le cadenas du destinataire (sa clé publique).

2.2 Déchiffrement du message : le destinataire ouvre le cadenas avec sa clé secrète (privée)

Le destinataire déchiffre automatiquement le message crypté car il possède la clé du cadenas (sa clé secrète).

3. Télécharger et installer OpenPGP

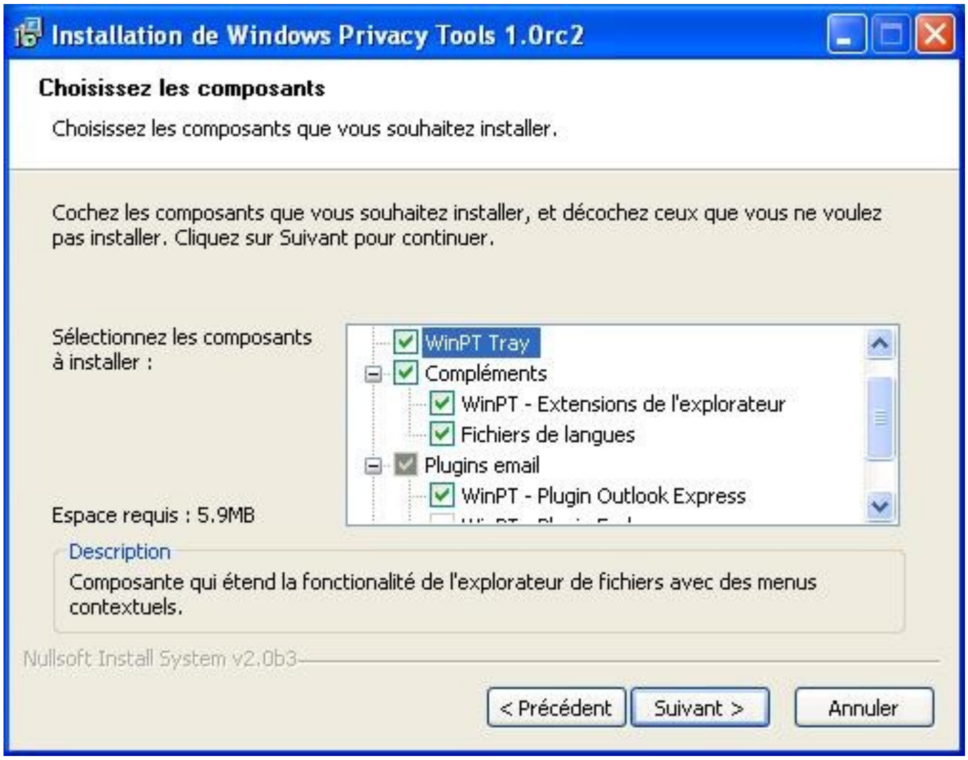
3.1 OpenPGP pour Windows

3.1.1 GPG : GNU Privacy Guard

WinPT−GPG
http://winpt.sourceforge.net/fr/download.php (WinPT + GPG)

+ Contient des plug−ins automatiques pour les e−mails (Outlook Express, Eudora)
+ Compatible avec PGP 6, 7, 8
+ Gratuit pour tous, et librement adaptable/modifiable par les entreprises ou les particuliers (licence GNU GPL)

− Traduction française partielle
− Peu de documentation



Installation de **WinPT−GPG** (Windows)

3.1.2 PGP© : Pretty Good Privacy

PGPfreeware 8.0
http://www.pgp.com/products/freeware.html

\+ Bonne ergonomie
\+ Documentation fournie (en anglais)

− Aucun plug−in automatique pour les e−mails
− Pas de traduction française (anglais seulement)
− Payant pour les entreprises et les professions libérales

3.2 OpenPGP pour MacOS X

3.2.1 MacGPG (Mac GNU Privacy Guard)

MacGPG
http://macgpg.sourceforge.net/fr/index.html (divers logiciels à installer)

\+ Accepte des plug−ins automatiques pour les e−mails
\+ Compatible avec PGP 6, 7, 8
\+ Gratuit pour tous, et librement adaptable/modifiable par les entreprises et les particuliers (licence GNU GPL)

− Traduction française partielle
− Peu de documentation

3.2.2 PGP© : Pretty Good Privacy

PGPfreeware 8.0
http://www.pgp.com/products/freeware.html

+ Bonne ergonomie
+ Documentation fournie (en anglais)

− Aucun plug−in automatique pour les e−mails
− Pas de traduction française (anglais seulement)
− Payant pour les entreprises et les professions libérales

3.3 OpenPGP pour Linux

GPG

(automatiquement installé dans toutes les distributions Linux)

3.4 OpenPGP pour les autres systèmes (MacOS 8/9, Palm, WindowsCE)

PGP© 2.6, PGP© 6.5, etc.

Voir une liste sur le site OpenPGP en français
http://openpgp.vie−privee.org/latest.html

4. Mise en place des clés PGP

Avant d'utiliser OpenPGP, il est nécessaire de se créer sa propre paire de clés et de se procurer la clé publique de ses correspondants.

4.1 Générer votre paire de clés

Cette paire de clés sera **unique** normalement, et vous pouvez la conserver durant des années. Donc, entrainez−vous avant de diffuser la clé publique issue de cette paire de clés.

GPG ou PGP© vous proposent de générer votre paire de clés lors du premier lancement.

Cette paire de clés contient une clé publique + une clé privée :

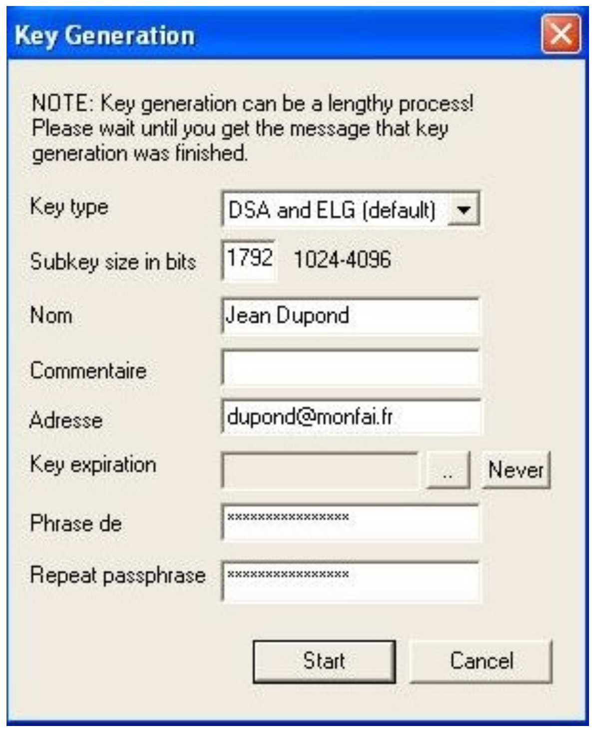
PAIRE DE CLÉS OpenPGP :

une clé publique (le cadenas)

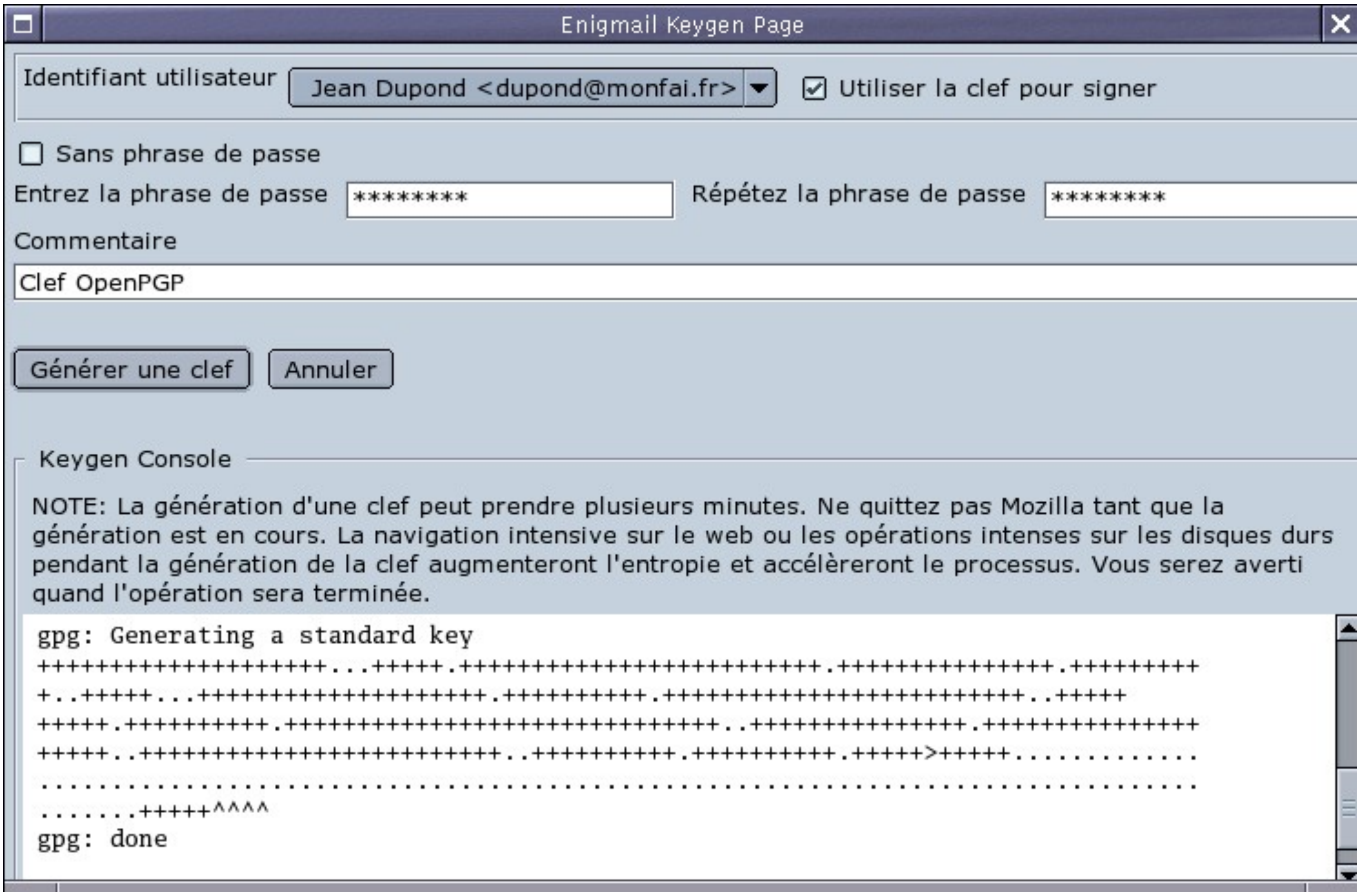
+

une clé privée (la clé ouvrant le cadenas)

Génération des clefs :



Génération de clef dans **WinPT−GPG** (Windows)



Génération de clef dans **Enigmail−Mozilla** (Windows, Linux, MacOS X)



Génération de clef dans **Kgpg (KDE)** (Linux)

4.2 Exporter votre clé publique et envoyer une copie de cette clé publique à vos correspondants

Cette clé publique est le "cadenas" qui permettra à vos correspondants de crypter les e−mails qu'ils vous envoient.

GPG ou PGP© permettent l'exportation de votre clé publique par leur fonction "export".

Ces correspondants doivent avoir une copie de votre clé publique PGP, qui ressemblera à ceci :


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.1 (GNU/Linux)

mQGiBD8rr14RBACE42tdHcXHDzM6quffREJIid0AxePj5sCUnvRsf211+VJjtbWp
XTmuVbOwWaXlXQ9fg8BhSulCwo/mPZoWF1PKgQzGDMDvYns4alX409obU0pwykQ9
dCf3QhI1p3mBT1A7Kfviqzyigqjg6xB+TYgDK2tWbyEYfwCk17Zu01xUZwCgkPJK
kbYAX4+0LoDEYCmrHIRqy3cD/jvPl4z2jdwaxRARwv6M/oKgFaA88dI/FIxo/aBJ
Coj7fvcSsszEF0ARyvIgbV6sD9LVwDX8L+Dwmsyfht6UxvwaH6fHZewEXbmGvcwg
Tw9uBEzctGlzdDco5nv6ldqIaZnDJkaVlDM61FfaSA30zZbKVTRdfWaCuQS4BErO
LatgA/kB3I6Fv4gGk9Z/HVaZdosrzu1THokTweSDVKay1Lt3grZNPTzbtTvyNvZp
7SDBUb140ysDQC/Zqy19iqkXp59eKwm2iw0z066LPc3lNu8ciekzwrWuwVLyNnS4
```

kyVBKC2928ILQy+2TF3whGxx+G0r+DKcxi1JVN+QjICH/ByzXbQeSmVhbiBEdXBv
bmQgPGR1cG9uZEBtb25mYWkuZnI+iFkEExECABkFAj8rr14ECwcDAgMVAgMDFgIB
Ah4BAheAAAoJENL6SLGOBr8HAIcAnjGhYIhPnoFUwo5xKZfcx4ZpX8uXAJ9lhDfm
zkZToy1aqM4sqh5497BGRLkBDQQ/K69iEAQA5Rw3BlKa11nPn+NeiZMydr6/FHZl
P5eo0VP1Tzmr6SO9NFKyLPsXxufBn+muTk6X/wehvDuMsKHkKHlPh9EIrLu8xO5w
Aln56aCEdZYdz31R2+WhImKUs0bR+NCLV8jdaVAu0R6KswHX3DDrfC2sPSuxaabp
tlydwe/goZpwcecABAsEAKNAF4i1HJfxRYII4gnJrvQWaCQmFJv+2AG7ERq4UHCd
eZLAagN5BOVHKXgmqAddH8qSP2VRZTGG1RThw7urGVVh4jd0OBuFs7anU4DVCKHz
2phNSCv2sRcq7qC/J6xHr3WRyiFn0BDhy8TOu6ceiTKST/Mdt8wpz+Y9u7oUT+J7
iEYEGBECAAYFAj8rr2IACgkQ0vpIsY4GvwcSrQCfQQowSwTy7U7/OVZMHqAUNhJp
fUwAn1Hptv3FNFYIo6lIa/+i4lwrMNVw
=S9md
-----END PGP PUBLIC KEY BLOCK-----

4.3 Importer la clé publique de vos correspondants pour la stocker dans votre "trousseau"

GPG ou PGP© permettent l'importation de la clé de vos correspondants dans votre trousseau de clés publiques par la fonction "import".

Ensuite, lorsque vous enverrez un e−mail à un de ces correspondants, le plug−in courrier se chargera de trouver le "cadenas" de ce correspondant (sa clé publique) dans votre trousseau de clés publiques PGP, puis il cryptera automatiquement le message avant envoi.

5. Utiliser OpenPGP

5.1 L'aspect technique : les plug−ins courrier

La façon la plus simple d'utiliser OpenPGP est d'installer un "plug−in" (une extension) : ce plug−in ajoute dans le logiciel e−mail une **icone OpenPGP** sur laquelle il suffira de cliquer pour crypter ou déchiffrer le message (ou signer et vérifier).

PGPfreeware 8.0 ne fournit pas de plug−ins courrier. Pour obtenir les plug−ins PGP© 8.0, il faut acquérir la version payante (voir http://www.pgpeurope.com). Les opérations de chiffrement peuvent cependant être réalisées dans PGPfreeware 8.0 par le presse−papiers ou la barre d'outils flottante (voir la FAQ ci−dessous).

Pour GPG, soit le plug−in est inclus (Outlook Express, Eudora), soit il faut télécharger le plug−in et l'installer, suivant le logiciel de courrier utilisé :

Windows

Outlook Express : inclus dans WinPT−GPG 1.0 (libre)

Eudora : inclus dans WinPT−GPG 1.0 (libre)

Thunderbird Mail : Enigmail (libre) http://enigmail.mozdev.org/thunderbird.html

Mozilla : Enigmail (libre) http://enigmail.mozdev.org/ (Voir **guide d'installation** http://openpgp.vie−privee.org/enigmail.html)

Outlook : G−Data (libre) http://www.gdata.de/gpg/download.html

Pegasus Mail : QDGPG (libre)http://community.wow.net/grt/qdgpg.html

The Bat! : Ritlabs (shareware) http://www.ritlabs.com/the_bat/pgp.html

Becky! 2 : BkGnuPG (freeware) http://hp.vector.co.jp/authors/VA023900/gpg−pin/index_en.html

Linux

KMail (KDE) : inclus dans KMail

Thunderbird Mail : Enigmail (libre)http://enigmail.mozdev.org/thunderbird.html

Mozilla : Enigmail (libre) http://enigmail.mozdev.org/ (Voir **guide d'installation** http://openpgp.vie−privee.org/enigmail.html)

Evolution (Gnome) : inclus dans Evolution

MacOS X

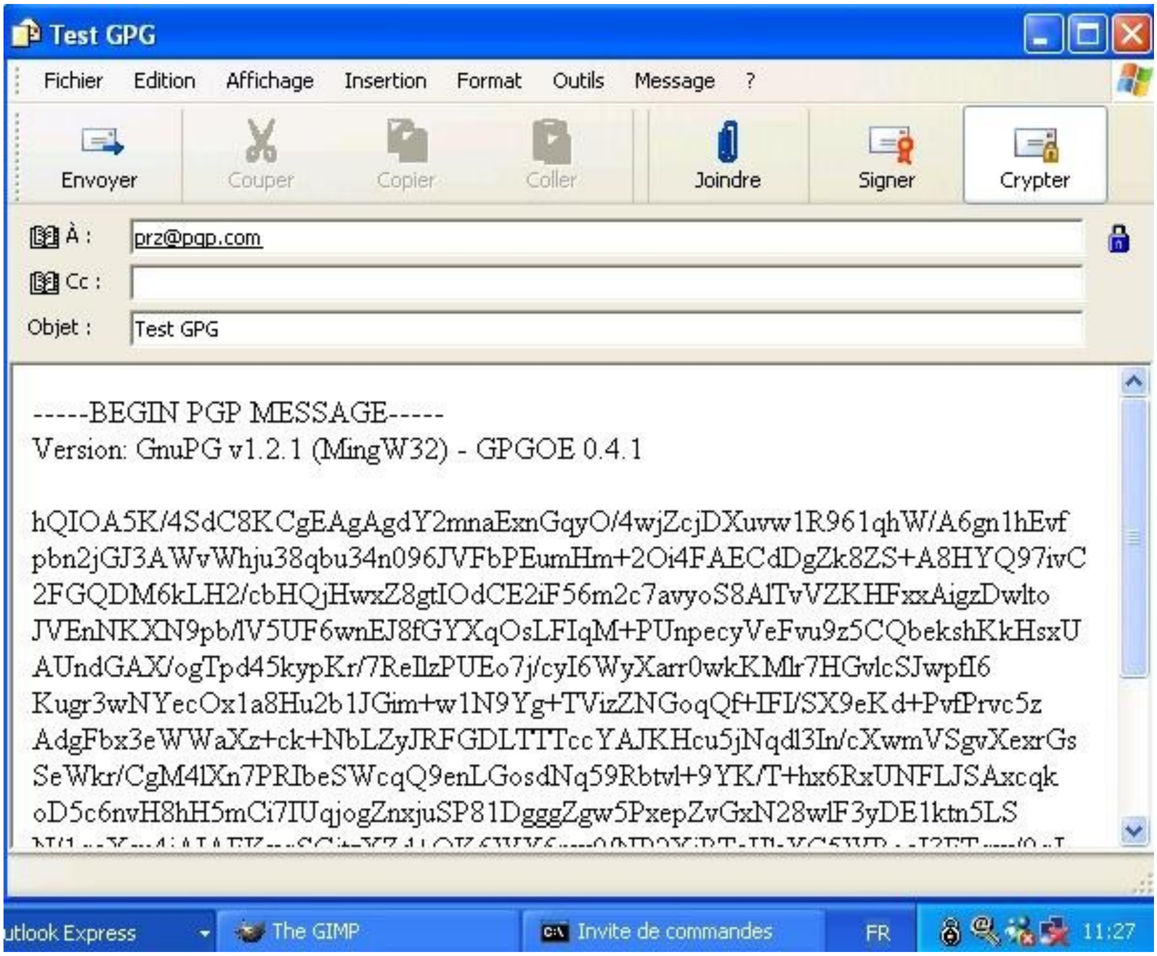
Apple Mail : GPGMail for OSX (libre) http://www.sente.ch/software/GPGMail/

Eudora : Eudora−GPG (libre) http://mywebpages.comcast.net/chang/EudoraGPG/

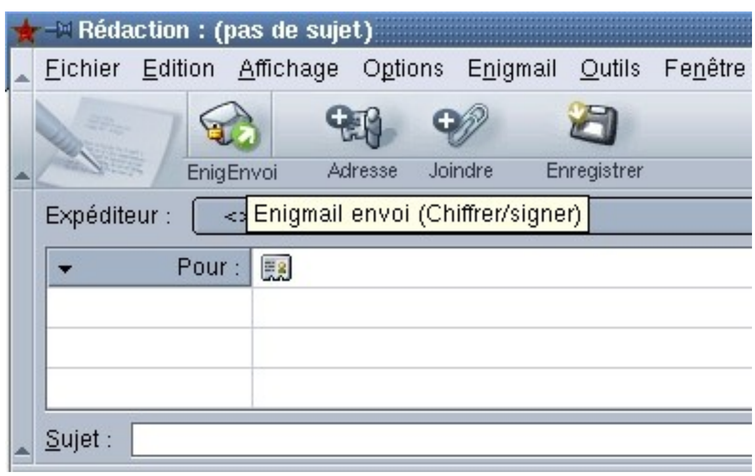
Entourage : EntourageGPG (libre) http://entouragegpg.sourceforge.net/fr_readme.html

Thunderbird Mail : Enigmail (libre)http://enigmail.mozdev.org/thunderbird.html

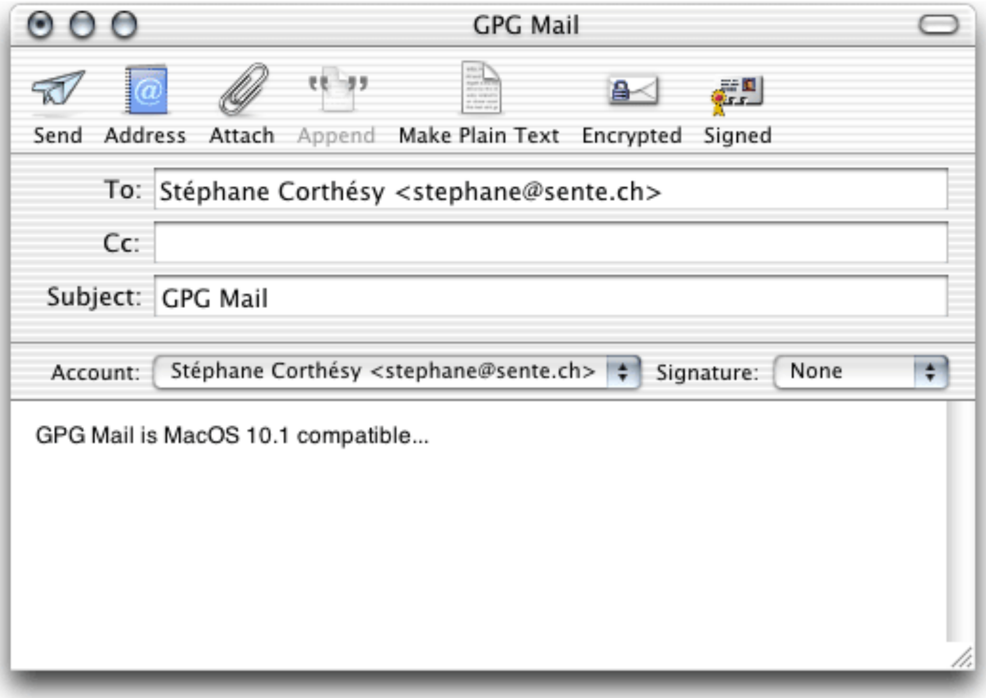
Mozilla : Enigmail (libre) http://enigmail.mozdev.org/ (Voir **guide d'installation** http://openpgp.vie−privee.org/enigmail.html)



GPG et le "plug−in" **GPGOE** pour Outlook Express (Windows)



GPG et le "plug−in" **Enigmail** pour Mozilla / Netscape 7



GPG et et le "plug−in" **GPGMail** pour Mail (MacOS X)

5.2 L'aspect humain : décider vos correspondants à crypter

Voir la première partie : "Pourquoi crypter vos e−mails ?"

6. Documentations

Site web de WinPT−GPG :
http://winpt.sourceforge.net/fr/index.php/

FAQ sur WinPT−GPG :
http://www.winpt.org/fr/faq.html

Mode d'emploi de MacGPG (MacOS X) :
http://www.gbronner.net/mail/GPGMacOSX.html

Guide d'installation Mozilla / Enigmail :
http://openpgp.vie−privee.org/enigmail.html

Mode d'emploi de GPG ligne de commande :

http://www.gnupg.org/gph/fr/manual.html

PGP© 8.0 pour Windows XP :
www.pgpsupport.com

Site web de GPG :
www.gnupg.org

International PGP© Home page :
www.pgpi.org

OpenPGP en français :
http://openpgp.vie−privee.org/

7. Foire Aux Questions sur OpenPGP

7.1 Pourquoi la clé PGP générée est une "paire" de clés ?

La clé publique est le **cadenas** : elle sert à crypter
La clé privée est la **clé** du cadenas : elle sert à déchiffrer

Ce qui a été crypté avec la clé PGP (publique) de monsieur X, ne peut être déchiffré que par la clé privée de monsieur X, qui est seul à la détenir.

Quand vous envoyez un message PGP à quelqu'un, ce message est crypté avec sa clé publique (et il le déchiffrera avec sa clé privée).

7.2 Le cryptage est−il automatique ?

Oui, à trois conditions :
1) que le plug−in GPG/PGP© correspondant au logiciel e−mail utilisé (par exemple Outlook Express ou Mozilla / Netscape 7) ait été installé;
2) que le destinataire possède déjà une clé publique PGP et vous l'ai envoyé;
3) que vous cliquiez sur l'icone "cryptage OpenPGP" de votre logiciel e−mail avant l'envoi.

7.3 Ai−je besoin de choisir un mot de passe pour crypter en PGP ?

Non, le e−mail est crypté par le "cadenas" du destinataire (sa clé publique).

Contrairement aux logiciels de cryptage habituels, l'élément qui sert à crypter est différent de celui qui sert à déchiffrer : c'est comme un coffre−fort qui devrait être fermé avec une clé n° 1 et rouvert avec une clé n°2,

chaque clé ne pouvant pas faire autre chose. Ici, la clé publique (ou "cadenas") sert à crypter et uniquement crypter.

7.4 Pourquoi OpenPGP me demande une "phrase de passe" ?

PGP demande au destinataire une "phrase de passe" pour utiliser la clé secrète de déchiffrement. Cette phrase de passe empêche quelqu'un qui touche à votre ordinateur de se servir à votre insu de votre clé privée.

C'est une double sécurité : même si quelqu'un réussissait à vous voler une copie de votre clé privée, il devrait encore entrer un code pour pouvoir s'en servir et déchiffrer les messages que vous recevez ou signer un message à votre place.

7.5 Suis−je obligé de crypter tous mes e−mails ?

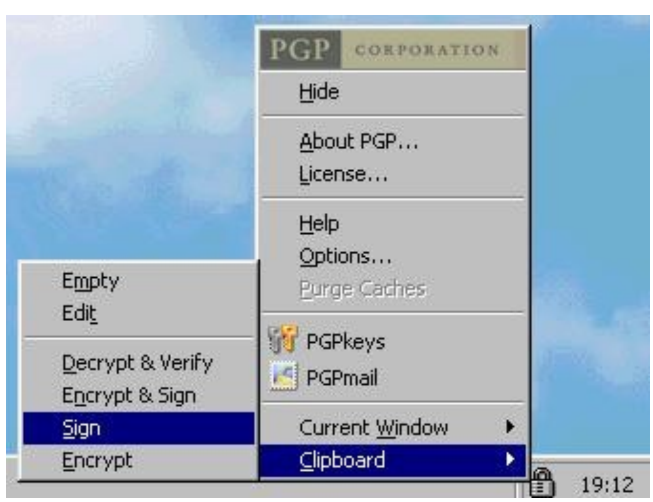
Dans l'idéal, oui. Sinon, cela met en évidence le caractère secret des rares e−mails cryptés, et surtout les noms de leur destinataire.

7.6 Si j'envoie un e−mail crypté à un destinataire qui n'utilise pas OpenPGP, que se passe−t−il ?

Ce cas de figure est théoriquement impossible : si le destinataire n'utilise pas OpenPGP, il n'a pas généré de paire de clés PGP, et n'a donc pas pu vous envoyer sa clé publique. OpenPGP crypte les e−mail à l'aide du "cadenas" du destinataire (sa clé publique PGP). Si OpenPGP ne trouve aucune clé publique correspondant au destinaire, il ne crypte pas.

7.7 Puis−je crypter un fichier sans l'envoyer ou avant de l'envoyer?

Oui, à l'aide de la fonction "Encrypt clipboard" (Crypter le presse−papiers) de GPG ou PGP©, qui cryptera la partie de texte mise en mémoire :



PGPfreeware 8.0 dans Windows 98



GPG dans Windows XP



La barre d'outils flottante de PGPfreeware 8.0

7.8 Puis−je crypter tout mon disque dur avec OpenPGP ?

En théorie, oui. Mais en pratique, OpenPGP est surtout un outil pour les e−mails, et il est mal adapté au cryptage de tout le disque.

L'outil PGPdisk est fourni dans la version payante de PGP©. Comme programmes gratuits, existent : sous Windows le logiciel **Scramdisk** http://www.samsimpson.com/scramdisk.php#dload (Windows 95/98/Me), sous Linux (Mandrake, SuSE, Knoppix) le **cryptage loopback** du disque http://openpgp.vie−privee.org/linux.html, et sous MacOSX 10.3 l'outil **FileVault** http://www.apple.com/fr/macosx/panther/file_vault.html.

8. Législation française

1. Principe : la réglementation des programmes informatiques de cryptographie

La France reste, pour des raisons assez incompréhensibles, la seule grande démocratie qui interdise aux citoyens de chiffrer en toute liberté leurs propres données privées ou leurs communications. Les multiples

lois et décrets actuellement en vigueur (notamment les lois du 29 décembre 1990 et du 10 juillet 1991, et les décrets du 24 février 1998 et du 17 mars 1999) ainsi que la future "Loi pour la confiance dans l'économie numérique" (projet de loi en 2003) posent le principe de la liberté d'utilisation des outils de cryptographie, mais soumettent dans le même temps ces outils à des régimes complexes de déclaration ou d'autorisation.

2. En pratique : autorisation des outils OpenPGP en France

GPG : en 2002, la FSF−France ("Free Software Foundation"), une association liée au mouvement des logiciels libres Linux, a déposé un dossier de demande d'autorisation auprès de l'administration compétente (la DCSSI), pour le logiciel GnuPG (GPG). Cette demande a été acceptée, rapidement et dans des conditions très larges. GPG 1.x est donc librement utilisable dans toutes ses fonctions en France par tous, particuliers comme entreprises.

PGP© : en 2000, la société Network Associates France, propriétaire à l'époque de PGP©, avait obtenu une autorisation de la DCSSI (alors SCSSI) pour PGP version 6.0.2. Il est difficile de savoir si cette autorisation concernait, comme GPG, également les versions futures (par exemple PGP 8.0.3). Pour plus de détails sur PGP©, consulter la DCSSI (voir site web plus bas).

Liens :
Autorisation de GPG accordée à la FSF
Site de la DCSSI (cache Google − site ssi.gouv.fr souvent injoignable)
Textes de lois et décrets (rechercher le terme "cryptologie")
Projet de Loi pour la confiance dans l'économie numérique
Les législations du monde entier

(*) Les termes scientifiques corrects sont "chiffrement", "déchiffrement", "chiffrer", "déchiffrer". "Décrypter" possède un sens précis en cryptologie et signifie "casser" le code. Cryptage et crypter n'existent pas (même si les dictionnaires leur reconnaissent un certain statut).

Rédaction :
pplf (http://openpgp.vie−privee.org/)
et les membres de la FIL (http://www.vie−privee.org)
